2019

FUNDAMENTALS OF CYBER LAWS AND ARTIFICIAL INTELLIGENCES

Compiled by: Mr. Rameswar Mishra

Rs. 100/-

Contents

Introduction of Cyber Law 3
Cyber Laws in India 4
History of Cyber law in India 4
Role of law in the Cyber world 5
Types of Cyber Crimes 6
Evolution of Cyber Law in India 7
The Need for Cyber Laws 7
The Information Technology Act, 2000 7
IT Amendment Act (ITA-2008) 8
Prevent Cyber Crime 9
Introduction of Artificial Intelligence (AI) 9
Reasoning, problem solving 11
Knowledge representation 11
Default reasoning 12
The breadth of commonsense knowledge 12
The subsymbolic form of some commonsense knowledge 13
Learning 14
Natural language processing 14
Perception 15
Motion and manipulation 16
Social intelligence 16
General intelligence 17
Approaches of AI 18
Tools of AI 18
There are four types of artificial intelligence 19
  - Reactive machines 19
  - Limited memory 19
  - Theory of mind 19
  - Self-awareness 19
Ethics of artificial intelligence 19
Robot ethics 19

Introduction of Cyber Law:

Information technology law (also called "cyberlaw") concerns the law of information technology, including computing and the internet. It is related to legal informatics, and governs the digital dissemination of both (digitalized) information and software, information security and electronic commerce. It has been described as "paper laws" for a "paperless environment". It raises specific issues of intellectual property in computing and online, contract law, privacy, freedom of expression, and jurisdiction.

IT law does not constitute a separate area of law rather it encompasses aspects of contract, intellectual property, privacy and data protection laws. Intellectual property is an important component of IT law, including copyright, rules on fair use, and special rules on copy protection for digital media, and circumvention of such schemes. The area of software patents is controversial, and still evolving in Europe and elsewhere. The related topics of software licenses, end user license agreements, free software licenses and open-source licenses can involve discussion of product liability, professional liability of individual developers, warranties, contract law, trade secrets and intellectual property. In various countries, areas of the computing and communication industries are regulated – often strictly – by governmental bodies.

There are rules on the uses to which computers and computer networks may be subjected to, in particular there are rules on unauthorized access, data privacy and spamming. There are also limits on the use of encryption and of equipment which may be used to defeat copy protection schemes. The export of hardware and software between certain states within the same country ,as in United States, is also controlled.[citation needed]

There are laws governing trade on the Internet, taxation, consumer protection, and advertising. There are laws on censorship versus freedom of expression, rules on public access to government information, and individual access to information held on them by private bodies. There are laws on what data must be retained for law enforcement, and what may not be gathered or retained, for privacy reasons. In certain circumstances and jurisdictions, computer communications may be used in evidence, and to establish contracts. New methods of tapping and surveillance made possible by computers have wildly differing rules on how they may be used by law enforcement bodies and as evidence in court.

Computerized voting technology, from polling machines to internet and mobile-phone voting, raise a host of legal issues. Some states limit access to the Internet, by law as well as by technical means.

The new boon brought by information technology has brought its scar in the form of cybercrime, moreover the new business environment required new regulations for its legal endorsement as more and more business communities are moving towards electronic commerce and trans-border contracts. To address this issue the United Nation through its core agency, United Nations Commission on International Trade Law (UNCITRAL) had formulated a model legislation on electronic commerce. The Information Technology Act 2000 is the prime legislation dealing with cyber offenses and electronic commerce in India which is based on the United Nations Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL).The Information Technology Act 2000 is applicable to the whole of India, including any offense committed outside India, if such contravention involves a computer, computer system or computer network located in India. India with the adoption of the Information Technology Act, 2000 has entered the coveted world of the few countries that have separate law to deal with information technology issues. This has paved way for the growth of e-commerce and e-transaction, thereby advancing economic growth and a new era of e-governance has come into existence which helps in bringing transparency, efficiency and accountability in governance.

Cyber Laws in India:

Cyber Laws in India prevent any crime done using technology, where a computer is a tool for cybercrime. The laws for cyber crime protects citizens from dispensing sensitive information to a stranger online. Ever since the introduction of cyber laws in India , IT Act 2000 was enacted and amended in 2008 covering different types of crimes under cyber law in India. The Act explains the types of cyber crime and punishment.

By definition, cyberlaw states that it's a subset of law which specifically deals with the inter-network technology. Meaning cyber law in India deals with the crimes done through a computer or any other digital device.

History of Cyber law in India:

The information Technology Act is an outcome of the resolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law. This resolution recommended, inter alia, that all states give favourable consideration to the said Model Law while revising ,enacting new law, so that uniformity may be observed in the laws, of the various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information.

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft. After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber crime and to facilitate speedy locating of a cyber criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. Finally, this suggestion was dropped by the IT Ministry in its final draft.

The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000.
With the passage of time, as technology developed further and new methods of committing crime using Internet & computers surfaced, the need was felt to amend the IT Act, 2000, to insert new kinds of cyber offences and plug in other loopholes that posed hurdles in the effective enforcement of the IT Act, 2000. This led to the passage of the Information Technology (Amendment) Act, 2008 which was made effective from 27 October 2009. The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts.

Role of law in the Cyber world:

- Cyber Crimes
- Electronic and Digital Signatures
- Intellectual Property
- Data Protection and Privacy

In cybercrime, the computer can either be a tool, target, or both.

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

- The Computer as a Target :-using a computer to attack other computers.
  e.g. Hacking,Virus/Worm attacks,DOS attack etc.
- The computer as a weapon :-using a computer to commit real world crimes.
  e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law ,in the way that property or contract are ,as it is ,an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Importance of Cyber Law in India:

Cyber laws in India or cybercrime law in India is important, because of the prime reason that cyber crime act in India encompasses and covers all the aspects which occur on or with the internet - transactions and activities which concern the internet and cyberspace.

Types of Cyber Crimes:

Different types of cyber crimes have different punishments in India.

- Identity theft - When personal information of a person is stolen with the purpose of using their financial resources or to take a loan or credit card in their name, then such a crime is known as Identity theft.
- Cyberbullying - When a teenager or adolescent harasses, defames, or intimidates someone with the use of the internet, phone, chat rooms, instant messaging or any other social network then the person is said to be committing the crime of Cyberbullying. When the same crime is done by adults it is known as Cyberstalking.
- Cyberterrorism - When a threat of extortion or any kind of harm is being subjected towards a person, organization, group or state, it is known as the crime of Cyber Terrorism. Generally, it includes the well-planned attack strategies on the Government and corporate computer system.
- Hacking - The most common cyber crime is Hacking. In this crime, the person gets access to other people's computers and passwords to use it for their own wrongful gain.

Evolution of Cyber Law in India:

With an increase in the dependency on the use of technology, the need for cyberlaw was necessary. Much like every coin has two sides, therefore, the dependency on technology has its pros and cons.

The rise of the 21st century marked the evolution of cyberlaw in India with the Information Technology Act, 2000 (popularly known as the IT Act). The first ever cyber crime was recorded in the year 1820[pdf].

The objective of Information Technology laws in India is as follows:

- To provide legal recognition for all e-transactions
- To give legal recognition to digital signatures as a valid signature to accept agreements online
- Protection of online privacy and stopping cyber crimes
- To give legal recognition to keeping accounting books in electronic form by bankers as well as other organizations
- The Indian IT law updated the Reserve Bank of India Act and the Indian Evidence Act.

With the evolution of cyber law almost all online activities came under scrutiny. However, one thing about cyber law is that there are certain areas on which cybercrime laws in India do not apply, such as:

- Negotiable Instrument being other than cheque
- Power of Attorney (PoA)
- Will
- The contract for Sale or Conveyance of Immovable Property
- Central Government notified documents or transactions

The Need for Cyber Laws:

In the present world which is more tech-savvy, the words cyber law and cyber crimes have also become more sophisticated.

Internet and technology were launched for research purposes and making life of humans easy but as the use and number of people on the internet increased, the need for cyber laws in India was felt.

As the nature of the internet is anonymous it is easy to commit cyber crimes. Thereby many could misuse this aspect largely.

The Information Technology Act, 2000:

When the emphasis was on the need for cyber law or cyber security laws, then, it was imperative to implement an IT law in India. Thus, the Information

Technology Act, 2000[1], or also known as the Indian Cyber Act or the Internet Law came to force in India. Since the enactment, the Indian Internet Laws were drafted to bring in view all the electronic records and online/electronic activities to legal recognition. The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Internet Laws in India not only validates digital signatures but also provides for how authentication of the documents, which has been accepted and generated by using the digital signatures, can be done.

As IT Act is a cyber security law introduced to secure cyberspace, the Information Technology Law was amended under;

- the Indian Penal Code
- the Indian Evidence Act
- the Banker's Book Evidence Act
- the Reserve Bank of India

The prime focus of cyber law in India is to prevent:

- computer crime
- forgery of electronic data & record in e-commerce
- electronic transaction

IT Amendment Act (ITA-2008):

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In). The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

IT Act, 2000 went through amendments[2]in the year 2008. These were made in light of the laws on cyber crime - IT Act, 2000 by way of the IT Act, 2008. They were enforced at the beginning of 2009 to strengthen the cyber security laws.

Modifications in the Information Technology Act, 2008 included the change in the definition of some terms such as communication device.

The amendment for the definition of communication device was to include:

- the current use
- to validate the digital signature
- to make the IP address owner accountable
- impose liability for data breaches

Prevent Cyber Crime:

No doubt that the cyber security laws or cyber laws in India provide protection from cyber crime. However, prevention is always better than cure. Therefore, one should take the following steps for preventing a cyber crime:

- Unsolicited text message - We all get text messages sometimes from unknown number. One should be cautious and try to avoid responding to text message or automated voice message from an unknown number.
- Downloads on the mobile phone - Download everything on the mobile phone from a trustworthy source only.
- Online buying - Always use a legitimate and trusted payment service. Hence, it's important to always use a credit card, because then, the charges can be disputed if there is a problem.
- Rating and feedback - Always check for seller’s rating and feedback of customer for the seller. Be sure that you are checking current feedbacks. Also, beware of feedbacks that are 100% seller favouring or have an entry on the same date.
- Personal Information Request - Everyone must have received a call or mail. In which, the person on the other side asks for personal information. This includes your card CVV or a mail containing an attachment, which requires you to click on embedded links. Be sure to never respond to such emails or calls.

Introduction of Artificial Intelligence (AI):

In computer science, artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans. Colloquially, the term "artificial intelligence" is often used to describe machines (or computers) that mimic "cognitive" functions that humans associate with the human mind, such as "learning" and "problem solving".

As machines become increasingly capable, tasks considered to require "intelligence" are often removed from the definition of AI, a phenomenon known as the AI effect. A quip in Tesler's Theorem says "AI is whatever hasn't been done yet." For instance, optical character recognition is frequently excluded from things considered to be AI, having become a routine technology. Modern machine capabilities generally classified as AI include successfully understanding human speech, competing at the highest level in strategic game systems (such as chess and Go), autonomously operating cars, intelligent routing in content delivery networks, and military simulations.

Artificial intelligence can be classified into three different types of systems: analytical, human-inspired, and humanized artificial intelligence. Analytical AI has only characteristics consistent with cognitive intelligence; generating a cognitive representation of the world and using learning based on past experience to inform future decisions. Human-inspired AI has elements from cognitive and emotional intelligence; understanding human emotions, in addition to cognitive elements, and considering them in their decision making. Humanized AI shows characteristics of all types of competencies (i.e., cognitive, emotional, and social intelligence), is able to be self-conscious and is self-aware in interactions. Artificial intelligence was founded as an academic discipline in 1956, and in the years since has experienced several waves of optimism, followed by disappointment and the loss of funding (known as an "AI winter"), followed by new approaches, success and renewed funding. For most of its history, AI research has been divided into subfields that often fail to communicate with each other. These sub-fields are based on technical considerations, such as particular goals (e.g. "robotics" or "machine learning"), the use of particular tools ("logic" or artificial neural networks), or deep philosophical differences. Subfields have also been based on social factors (particular institutions or the work of particular researchers).

The traditional problems (or goals) of AI research include reasoning, knowledge representation, planning, learning, natural language processing, perception and the ability to move and manipulate objects. General intelligence is among the field's long-term goals. Approaches include statistical methods, computational intelligence, and traditional symbolic AI. Many tools are used in AI, including versions of search and mathematical optimization, artificial neural networks, and methods based on statistics, probability and economics. The AI field draws upon computer science, information engineering, mathematics, psychology linguistics, philosophy, and many other fields. The field was founded on the claim that human intelligence "can be so precisely described that a machine can be made to simulate it". This raises philosophical arguments about the nature of the mind and the ethics of creating artificial beings endowed with human-like intelligence which are issues that have been explored by myth, fiction and philosophy since antiquity. Some people also consider AI to be a danger to humanity, if it progresses unabated. Others believe that AI, unlike previous technological revolutions, will create a risk of mass unemployment.

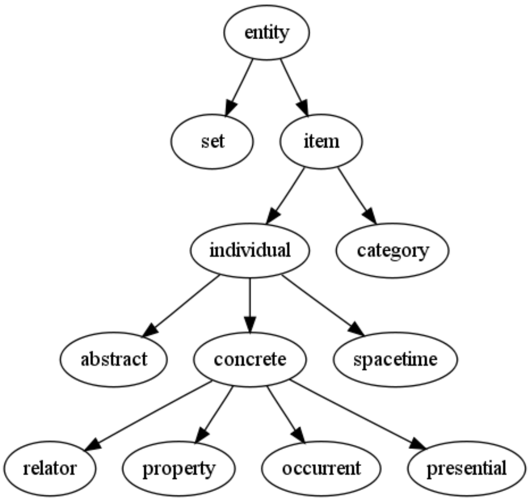
In the twenty-first century, AI techniques have experienced a resurgence following concurrent advances in computer power, large amounts of data, and theoretical understanding; and AI techniques have become an essential part of the technology industry, helping to solve many challenging problems in computer science, software engineering and operations research.

Artificial intelligence (AI),is the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience. The overall research goal of artificial intelligence is to create technology that allows computers and machines to function in an intelligent manner. The general problem of simulating (or creating) intelligence has been broken down into sub-problems. These consist of particular traits or capabilities that researchers expect an intelligent system to display. The traits described below have received the most attention.

Reasoning, problem solving→

Early researchers developed algorithms that imitated step-by-step reasoning that humans use when they solve puzzles or make logical deductions. By the late 1980s and 1990s, AI research had developed methods for dealing with uncertain or incomplete information, employing concepts from probability and economics. These algorithms proved to be insufficient for solving large reasoning problems, because they experienced a "combinatorial explosion": they became exponentially slower as the problems grew larger. In fact, even humans rarely use the step-by-step deduction that early AI research was able to model. They solve most of their problems using fast, intuitive judgements.

Knowledge representation→



An ontology represents knowledge as a set of concepts within a domain and the relationships between those concepts ,knowledge representation and knowledge engineering are central to classical AI research. Some "expert systems" attempt to gather together explicit knowledge possessed by experts in some narrow domain. In addition, some projects attempt to gather the "commonsense knowledge" known to the average person into a database containing extensive knowledge about the world. Among the things a comprehensive commonsense knowledge base would contain are: objects, properties, categories and relations between objects; situations, events, states and time; causes and effects; knowledge about knowledge (what we know about what other people know); and many other, less well researched domains. A representation of "what exists" is an ontology: the set of objects, relations, concepts, and properties formally described so that software agents can interpret them. The semantics of these are captured as description logic concepts, roles, and individuals, and typically implemented as classes, properties, and individuals in the Web Ontology Language. The most general ontologies are called upper ontologies, which attempt to provide a foundation for all other knowledge by acting as mediators between domain ontologies that cover specific knowledge about a particular knowledge domain (field of interest or area of concern). Such formal knowledge representations can be used in content-based indexing and retrieval, scene interpretation, clinical decision support, knowledge discovery (mining "interesting" and actionable inferences from large databases), and other areas.

Among the most difficult problems in knowledge representations are:

Default reasoning and the qualification problem-

Many of the things people know take the form of "working assumptions". For example, if a bird comes up in conversation, people typically picture an animal that is fist-sized, sings, and flies. None of these things are true about all birds. John McCarthy identified this problem in 1969 as the qualification problem: for any commonsense rule that AI researchers care to represent, there tend to be a huge number of exceptions. Almost nothing is simply true or false in the way that abstract logic requires. AI research has explored a number of solutions to this problem.

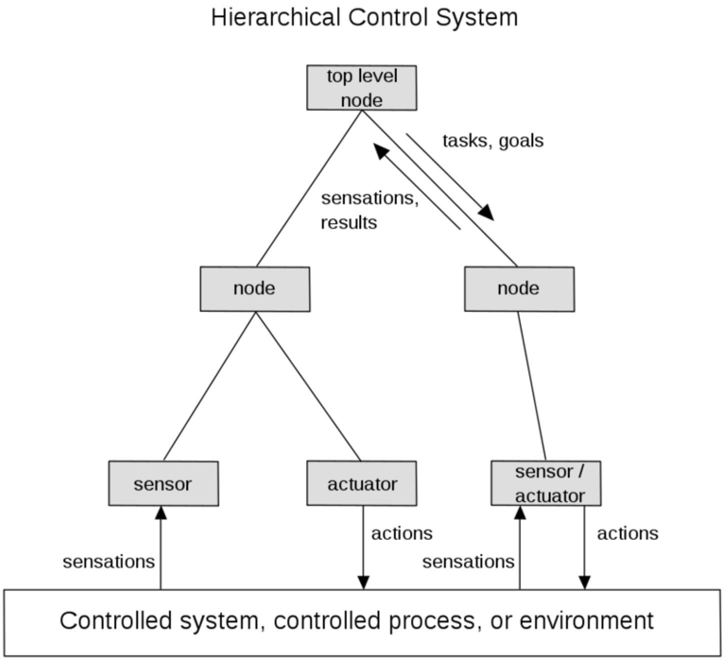
The breadth of commonsense knowledge-

The number of atomic facts that the average person knows is very large. Research projects that attempt to build a complete knowledge base of commonsense knowledge (e.g., Cyc) require enormous amounts of laborious ontological engineering—they must be built, by hand, one complicated concept at a time.

The subsymbolic form of some commonsense knowledge-

Much of what people know is not represented as "facts" or "statements" that they could express verbally. For example, a chess master will avoid a particular chess position because it "feels too exposed" or an art critic can take one look at a statue and realize that it is a fake. These are non-conscious and sub-symbolic intuitions or tendencies in the human brain. Knowledge like this informs, supports and provides a context for symbolic, conscious knowledge. As with the related problem of sub-symbolic reasoning, it is hoped that situated AI, computational intelligence, or statistical AI will provide ways to represent this kind of knowledge.

Planning→



A hierarchical control system is a form of control system in which a set of devices and governing software is arranged in a hierarchy. Intelligent agents must be able to set goals and achieve them. They need a way to visualize the future—a representation of the state of the world and be able to make predictions about how their actions will change it—and be able to make choices that maximize the utility (or "value") of available choices.

In classical planning problems, the agent can assume that it is the only system acting in the world, allowing the agent to be certain of the consequences of its actions. However, if the agent is not the only actor, then it requires that the agent can reason under uncertainty. This calls for an agent that can not only assess its environment and make predictions, but also evaluate its predictions and adapt based on its assessment.

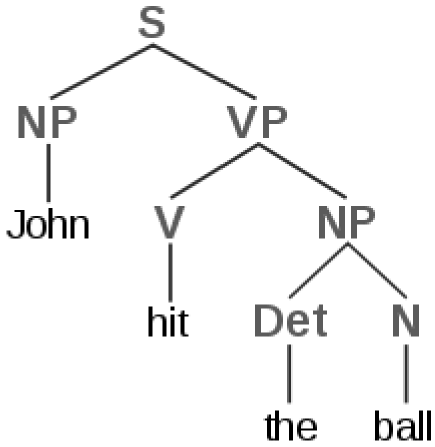
Multi-agent planning uses the cooperation and competition of many agents to achieve a given goal. Emergent behavior such as this is used by evolutionary algorithms and swarm intelligence.

Learning→

Machine learning (ML), a fundamental concept of AI research since the field's inception, is the study of computer algorithms that improve automatically through experience.

Unsupervised learning is the ability to find patterns in a stream of input, without requiring a human to label the inputs first. Supervised learning includes both classification and numerical regression, which requires a human to label the input data first. Classification is used to determine what category something belongs in, and occurs after a program sees a number of examples of things from several categories. Regression is the attempt to produce a function that describes the relationship between inputs and outputs and predicts how the outputs should change as the inputs change. Both classifiers and regression learners can be viewed as "function approximators" trying to learn an unknown (possibly implicit) function; for example, a spam classifier can be viewed as learning a function that maps from the text of an email to one of two categories, "spam" or "not spam". Computational learning theory can assess learners by computational complexity, by sample complexity (how much data is required), or by other notions of optimization. In reinforcement learning the agent is rewarded for good responses and punished for bad ones. The agent uses this sequence of rewards and punishments to form a strategy for operating in its problem space.

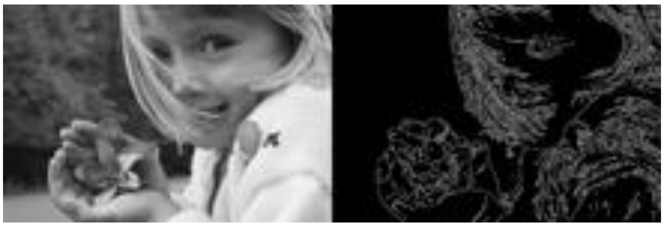
Natural language processing→



A parse tree represents the syntactic structure of a sentence according to some formal grammar.

Natural language processing (NLP) gives machines the ability to read and understand human language. A sufficiently powerful natural language processing system would enable natural-language user interfaces and the acquisition of knowledge directly from human-written sources, such as newswire texts. Some straightforward applications of natural language processing include information retrieval, text mining, question answering and machine translation. Many current approaches use word co-occurrence frequencies to construct syntactic representations of text. "Keyword spotting" strategies for search are popular and scalable but dumb; a search query for "dog" might only match documents with the literal word "dog" and miss a document with the word "poodle". "Lexical affinity" strategies use the occurrence of words such as "accident" to assess the sentiment of a document. Modern statistical NLP approaches can combine all these strategies as well as others, and often achieve acceptable accuracy at the page or paragraph level, but continue to lack the semantic understanding required to classify isolated sentences well. Besides the usual difficulties with encoding semantic commonsense knowledge, existing semantic NLP sometimes scales too poorly to be viable in business applications. Beyond semantic NLP, the ultimate goal of "narrative" NLP is to embody a full understanding of commonsense reasoning.

Perception→



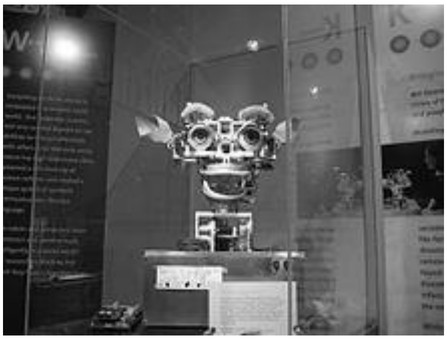
Feature detection (pictured: edge detection) helps AI compose informative abstract structures out of raw data.

Machine perception is the ability to use input from sensors ,such as cameras (visible spectrum or infrared), microphones, wireless signals, and active sonar, radar, and tactile sensors to deduce aspects of the world. Applications include speech recognition, facial recognition, and object recognition. Computer vision is the ability to analyze visual input. Such input is usually ambiguous; a giant, fifty-meter-tall pedestrian far away may produce exactly the same pixels as a nearby normal-sized pedestrian, requiring the AI to judge the relative likelihood and reasonableness of different interpretations, for example by using its "object model" to assess that fifty-meter pedestrians do not exist.

Motion and manipulation→

AI is heavily used in robotics. Advanced robotic arms and other industrial robots, widely used in modern factories, can learn from experience how to move efficiently despite the presence of friction and gear slippage. A modern mobile robot, when given a small, static, and visible environment, can easily determine its location and map its environment; however, dynamic environments, such as (in endoscopy) the interior of a patient's breathing body, pose a greater challenge. Motion planning is the process of breaking down a movement task into "primitives" such as individual joint movements. Such movement often involves compliant motion, a process where movement requires maintaining physical contact with an object. Moravec's paradox generalizes that low-level sensorimotor skills that humans take for granted are, counterintuitively, difficult to program into a robot; the paradox is named after Hans Moravec, who stated in 1988 that "it is comparatively easy to make computers exhibit adult level performance on intelligence tests or playing checkers, and difficult or impossible to give them the skills of a one-year-old when it comes to perception and mobility". This is attributed to the fact that, unlike checkers, physical dexterity has been a direct target of natural selection for millions of years.

Social intelligence→



Kismet, a robot with rudimentary social skills

Moravec's paradox can be extended to many forms of social intelligence. Distributed multi-agent coordination of autonomous vehicles remains a difficult problem. Affective computing is an interdisciplinary umbrella that comprises systems which recognize, interpret, process, or simulate human affects. Moderate successes related to affective computing include textual sentiment analysis and, more recently, multimodal affect analysis wherein AI classifies the affects displayed by a videotaped subject.

In the long run, social skills and an understanding of human emotion and game theory would be valuable to a social agent. Being able to predict the actions of others by understanding their motives and emotional states would allow an agent to make better decisions. Some computer systems mimic human emotion and expressions to appear more sensitive to the emotional dynamics of human interaction, or to otherwise facilitate human–computer interaction. Similarly, some virtual assistants are programmed to speak conversationally or even to banter humorously; this tends to give naïve users an unrealistic conception of how intelligent existing computer agents actually are.

General intelligence→

Historically, projects such as the Cyc knowledge base (1984–) and the massive Japanese Fifth Generation Computer Systems initiative (1982–1992) attempted to cover the breadth of human cognition. These early projects failed to escape the limitations of non-quantitative symbolic logic models and, in retrospect, greatly underestimated the difficulty of cross-domain AI. Nowadays, the vast majority of current AI researchers work instead on tractable "narrow AI" applications (such as medical diagnosis or automobile navigation). Many researchers predict that such "narrow AI" work in different individual domains will eventually be incorporated into a machine with artificial general intelligence (AGI), combining most of the narrow skills mentioned in this article and at some point even exceeding human ability in most or all these areas. Many advances have general, cross-domain significance. One high-profile example is that DeepMind in the 2010s developed a "generalized artificial intelligence" that could learn many diverse Atari games on its own, and later developed a variant of the system which succeeds at sequential learning. Besides transfer learning, hypothetical AGI breakthroughs could include the development of reflective architectures that can engage in decision-theoretic metareasoning, and figuring out how to "slurp up" a comprehensive knowledge base from the entire unstructured Web. Some argue that some kind of (currently-undiscovered) conceptually straightforward, but mathematically difficult, "Master Algorithm" could lead to AGI. Finally, a few "emergent" approaches look to simulating human intelligence extremely closely, and believe that anthropomorphic features like an artificial brain or simulated child development may someday reach a critical point where general intelligence emerges. Many of the problems in this article may also require general intelligence, if machines are to solve the problems as well as people do. For example, even specific straightforward tasks, like machine translation, require that a machine read and write in both languages, follow the author's argument (reason), know what is being talked about (knowledge), and faithfully reproduce the author's original intent (social intelligence). A problem like machine translation is considered "AI-complete", because all of these problems need to be solved simultaneously in order to reach human-level machine performance.

Approaches of AI:

- Cybernetics and brain simulation
- Symbolic
- Cognitive simulation
- Logic-based
- Anti-logic or scruffy
- Knowledge-based
- Sub-symbolic
- Embodied intelligence
- Computational intelligence and soft computing
- Statistical learning
- Integrating the approaches
- Intelligent agent paradigm
- Agent architectures and cognitive architectures

Tools of AI :

AI has developed a large number of tools to solve the most difficult problems in computer science. A few of the most general of these methods are discussed below:

- Search and optimization
- Logic
- Probabilistic methods for uncertain reasoning
- Classifiers and statistical learning methods
- Artificial neural networks
- Deep feedforward neural networks
- Deep recurrent neural networks
- Evaluating progress
- Applications:
- Healthcare
- Automotive
- Finance and economics
- Government
- Video games
- Military
- Audit
- Advertising
- Art

There are four types of artificial intelligence:

- Reactive machines
- Limited memory
- Theory of mind
- Self-awareness

Ethics of artificial intelligence→

The ethics of artificial intelligence is the part of the ethics of technology specific to robots and other artificially intelligent beings. It is typically divided into roboethics, a concern with the moral behavior of humans as they design, construct, use and treat artificially intelligent beings, and machine ethics, which is concerned with the moral behavior of artificial moral agents (AMAs).

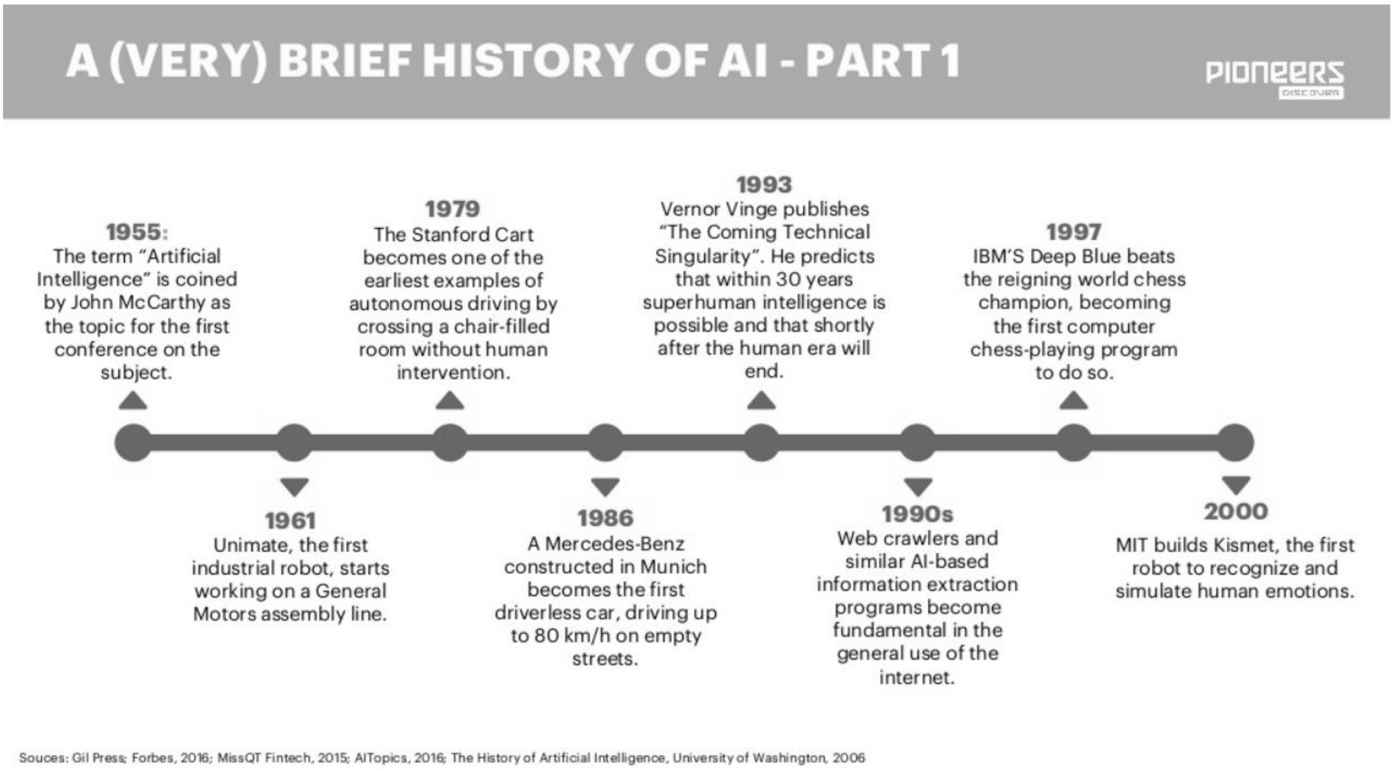
Robot ethics→

The term "robot ethics" (sometimes "roboethics") refers to the morality of how humans design, construct, use and treat robots and other artificially intelligent beings. It considers both how artificially intelligent beings may be used to harm humans and how they may be used to benefit humans.

AI cybersecurity tools can enable organizations to improve data security by detecting and thwarting potential threats through automated systems that continuously monitor network behavior and identify network abnormalities.

CYBER LAWS:

HISTORY OF ARTIFICIAL INTELLIGENCES (AI):



A (VERY) BRIEF HISTORY OF AI - PART 1

1955: The term "Artificial Intelligence" is coined by John McCarthy as the topic for the first conference on the subject.

1961 Unimate, the first industrial robot, starts working on a General Motors assembly line.

1979 The Stanford Cart becomes one of the earliest examples of autonomous driving by crossing a chair-filled room without human intervention.

1986 A Mercedes-Benz constructed in Munich becomes the first driverless car, driving up to 80 km/h on empty streets.

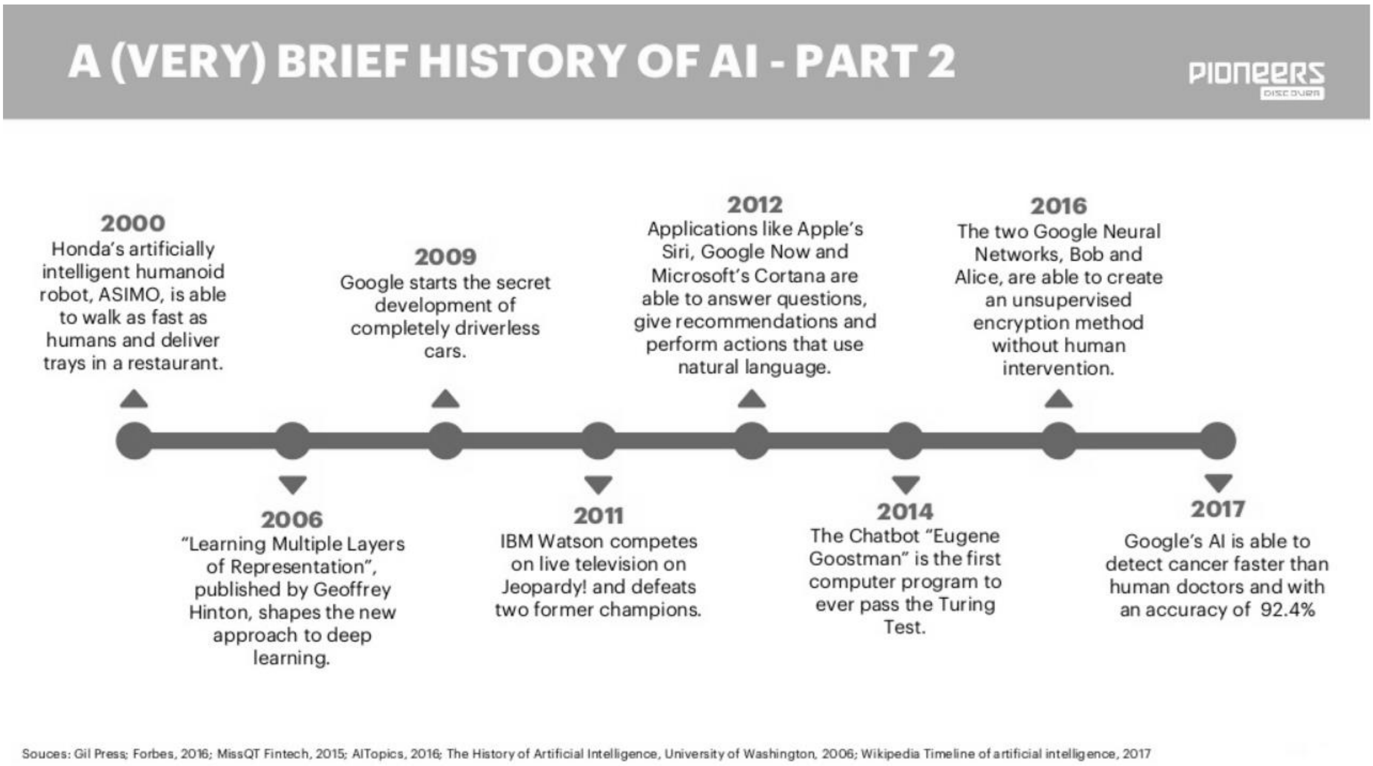
1993 Vernor Vinge publishes "The Coming Technical Singularity". He predicts that within 30 years superhuman intelligence is possible and that shortly after the human era will end.

1990s Web crawlers and similar AI-based information extraction programs become fundamental in the general use of the internet.

1997 IBM'S Deep Blue beats the reigning world chess champion, becoming the first computer chess-playing program to do so.

2000 MIT builds Kismet, the first robot to recognize and simulate human emotions.

Souces: Gil Press; Forbes, 2016; MissQT Fintech, 2015; AITopics, 2016; The History of Artificial Intelligence, University of Washington, 2006



A (VERY) BRIEF HISTORY OF AI - PART 2

2000 Honda's artificially intelligent humanoid robot, ASIMO, is able to walk as fast as humans and deliver trays in a restaurant.

2006 "Learning Multiple Layers of Representation", published by Geoffrey Hinton, shapes the new approach to deep learning.

2009 Google starts the secret development of completely driverless cars.

2011 IBM Watson competes on live television on Jeopardy! and defeats two former champions.

2012 Applications like Apple's Siri, Google Now and Microsoft's Cortana are able to answer questions, give recommendations and perform actions that use natural language.

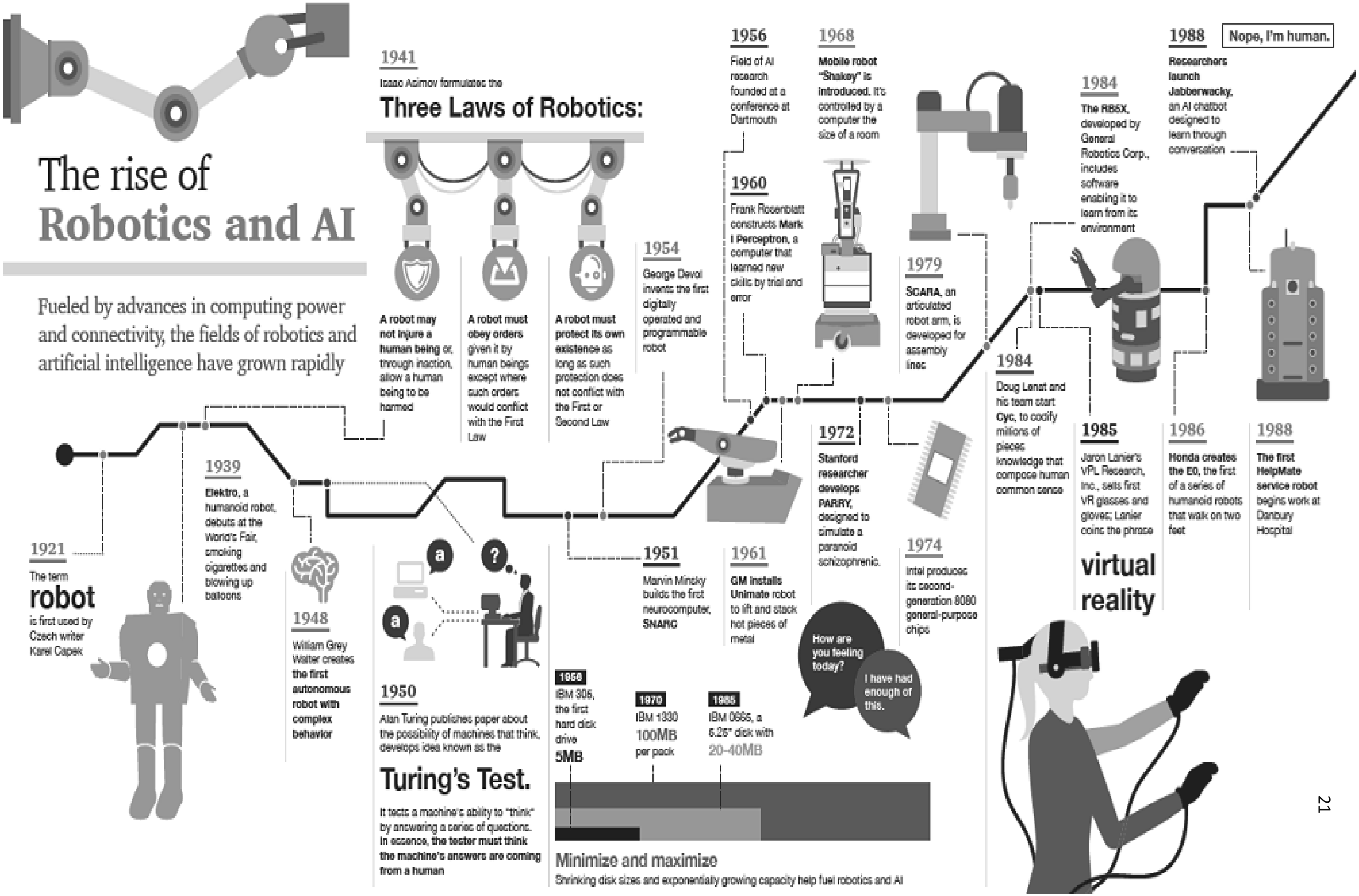
2014 The Chatbot "Eugene Goostman" is the first computer program to ever pass the Turing Test.

2016 The two Google Neural Networks, Bob and Alice, are able to create an unsupervised encryption method without human intervention.

2017 Google's AI is able to detect cancer faster than human doctors and with an accuracy of 92.4%

Souces: Gil Press; Forbes, 2016; MissQT Fintech, 2015; AITopics, 2016; The History of Artificial Intelligence, University of Washington, 2006; Wikipedia Timeline of artificial intelligence, 2017

RISE OF ROBOTICS:



The rise of Robotics and AI

Fueled by advances in computing power and connectivity, the fields of robotics and artificial intelligence have grown rapidly

1921
The term
robot
is first used by Czech writer Karel Capek

1939
Elektro, a humanoid robot, debuts at the World's Fair, smoking cigarettes and blowing up balloons

1941
Isaac Asimov formulates the

Three Laws of Robotics:

- **A robot may not injure a human being** or, through inaction, allow a human being to be harmed
- **A robot must obey orders** given it by human beings except where such orders would conflict with the First Law
- **A robot must protect its own existence** as long as such protection does not conflict with the First or Second Law

1948
William Grey Walter creates **the first autonomous robot with complex behavior**

1950
Alan Turing publishes paper about the possibility of machines that think, develops idea known as the

Turing's Test.

It tests a machine's ability to "think" by answering a series of questions. In essence, the tester must think **the machine's answers are coming from a human**

1951
Marvin Minsky builds the first neurocomputer, **SNARC**

1954
George Devol invents the first digitally operated and programmable robot

1956
Field of AI research founded at a conference at Dartmouth

1960
Frank Rosenblatt constructs **Mark I Perceptron**, a computer that learned new skills by trial and error

1961
GM installs Unimate robot to lift and stack hot pieces of metal

1968
Mobile robot "Shakey" is introduced. It's controlled by a computer the size of a room

1972
Stanford researcher develops PARRY, designed to simulate a paranoid schizophrenic.

1974
Intel produces its second-generation 8080 general-purpose chips

1979
SCARA, an articulated robot arm, is developed for assembly lines

1984
Doug Lenat and his team start **Cyc**, to codify millions of pieces knowledge that compose human common sense

1984
The RB5X, developed by General Robotics Corp., includes software enabling it to learn from its environment

1985
Jaron Lanier's VPL Research, Inc., sells first VR glasses and gloves; Lanier coins the phrase

virtual reality

1986
Honda creates the E0, the first of a series of humanoid robots that walk on two feet

1988
Researchers launch Jabberwacky, an AI chatbot designed to learn through conversation

Nope, I'm human.

1988
The first HelpMate service robot begins work at Danbury Hospital

1956
IBM 305, the first hard disk drive
5MB

1970
IBM 1330
100MB
per pack

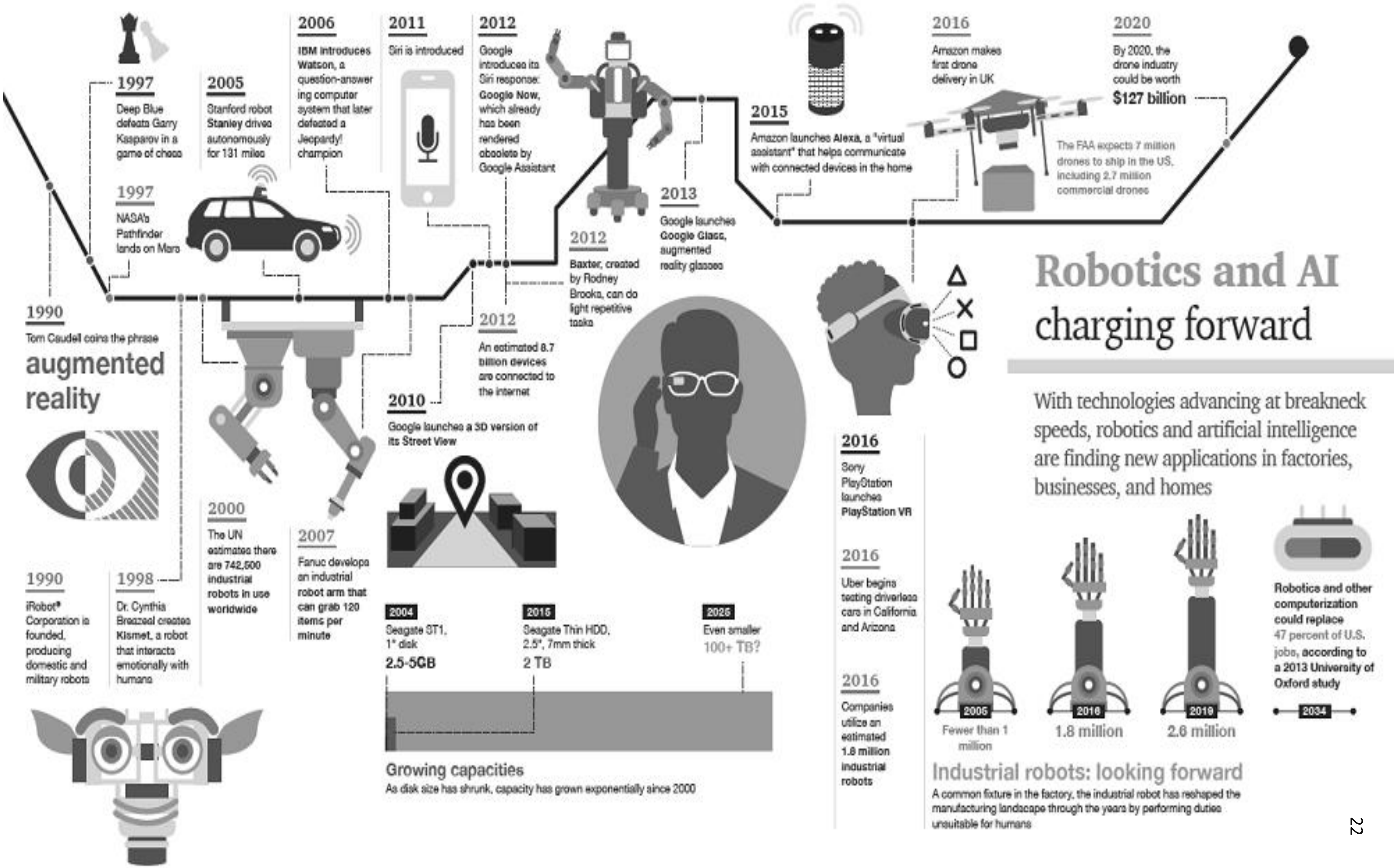
1985
IBM 0665, a 5.25" disk with
20-40MB

Minimize and maximize

Shrinking disk sizes and exponentially growing capacity help fuel robotics and AI

Robotics and AI charging forward

With technologies advancing at breakneck speeds, robotics and artificial intelligence are finding new applications in factories, businesses, and homes



1990
Tom Caudell coins the phrase
augmented reality

1990
iRobot® Corporation is founded, producing domestic and military robots

1997
Deep Blue defeats Garry Kasparov in a game of chess

1997
NASA's Pathfinder lands on Mars

1998
Dr. Cynthia Breazeal creates Kismet, a robot that interacts emotionally with humans

2000
The UN estimates there are 742,500 industrial robots in use worldwide

2005
Stanford robot Stanley drives autonomously for 131 miles

2006
IBM introduces Watson, a question-answering computer system that later defeated a Jeopardy! champion

2007
Fanuc develops an industrial robot arm that can grab 120 items per minute

2010
Google launches a 3D version of its Street View

2011
Siri is introduced

2012
Google introduces its Siri response: Google Now, which already has been rendered obsolete by Google Assistant

2012
An estimated 8.7 billion devices are connected to the internet

2012
Baxter, created by Rodney Brooks, can do light repetitive tasks

2013
Google launches Google Glass, augmented reality glasses

2015
Amazon launches Alexa, a "virtual assistant" that helps communicate with connected devices in the home

2016
Amazon makes first drone delivery in UK

2016
Sony PlayStation launches PlayStation VR

2016
Uber begins testing driverless cars in California and Arizona

2016
Companies utilize an estimated 1.8 million industrial robots

2020
By 2020, the drone industry could be worth **$127 billion**

The FAA expects 7 million drones to ship in the US, including 2.7 million commercial drones

Growing capacities

As disk size has shrunk, capacity has grown exponentially since 2000

2004
Seagate ST1, 1" disk
2.5-5GB

2015
Seagate Thin HDD, 2.5", 7mm thick
2 TB

2025
Even smaller
100+ TB?

Industrial robots: looking forward

A common fixture in the factory, the industrial robot has reshaped the manufacturing landscape through the years by performing duties unsuitable for humans

2005
Fewer than 1 million

2016
1.8 million

2019
2.6 million

2034
Robotics and other computerization could replace 47 percent of U.S. jobs, according to a 2013 University of Oxford study

Note

FUNDAMENTALS
OF
CYBER LAWS AND
ARTIFICIAL INTELLIGENCES

Name: Mr. Rameswar Mishra
Email Address: rameswarm35@gmail.com
Mobile Number: 09439425882/07077235390